Downloaded from orbit.dtu.dk on: May 05, 2023

DTU Library

The minimum number of minimal codewords in an [n,k]-code and in graphic codes

Alahmadi, A.; Aldred, R.E.L.; de la Cruz, R.; Ok, Seongmin; Solé, P.; Thomassen, Carsten

Published in:
Discrete Applied Mathematics

Link to article, DOI:
10.1016/j.dam.2014.11.015

Publication date:
2015

Document Version
Peer reviewed version

Link back to DTU Orbit

Citation (APA):
Alahmadi, A., Aldred, R. E. L., de la Cruz, R., Ok, S., Solé, P., & Thomassen, C. (2015). The minimum number of minimal codewords in an [n,k]-code and in graphic codes. *Discrete Applied Mathematics*, *184*, 32-39. https://doi.org/10.1016/j.dam.2014.11.015

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

THE MINIMUM NUMBER OF MINIMAL CODEWORDS IN AN $[n,k]-$CODE AND IN GRAPHIC CODES

A. ALAHMADI, R.E.L. ALDRED[1], R. DELA CRUZ, S. OK, P. SOLÉ, AND C. THOMASSEN

Abstract. We survey some lower bounds on the function in the title based on matroid theory and address the following problem by Dosa, Szalkai, Laflamme [9]: Determine the smallest number of circuits in a loopless matroid with no parallel elements and with a given size and rank. In the graphic 3-connected case we provide a lower bound which is a product of a linear function of the number of vertices and an exponential function of the average degree. We also prove that, for $p \geq 38$, every 3-connected graph with p vertices has at least as many cycles as the wheel with p vertices.

1. Introduction

Consider a binary linear code C of length n and dimension k. A codeword of C is called *minimal* if its support (non-zero entries) does not properly contain the support of another nonzero codeword. This concept was considered independently in code-based secret sharing schemes [4] and also in the study of the Voronoi domain of a code in the context of decoding [1]. Let $M(C)$ denote the number of minimal codewords of a code C. We consider the following natural question.

What is the minimum value of $M(C)$ for a code C of given length and dimension?

Equivalently, what is the minimum number of circuits (minimal dependent sets) in a binary matroid? If G is a graph, then the set of all subsets of edges may be thought of as a vector space over the field with two elements where addition is the symmetric difference. The *cycle space* $Z(G)$ is the subspace generated by the cycles. The cycle space of a graph G clearly forms a code called the *c*ycle code of G. When C is the cycle code of a graph the question amounts to finding the minimum number of cycles this graph can have. In [2] this problem was essentially solved for cubic 3-connected graphs. A graph can also be associated with a *g*raphic matroid, the matroid defined on the edge set of a graph such that the independent sets are the sets forming a forest. Hence, the circuits of the graphic matroid are the edge sets of the cycles in the graph. The more general question of finding the minimum number of circuits in a matroid was raised in [9].

Let $\mathbf{C}[n,k]$ denote the set of all $[n,k]$ codes with distance at least three (the motivation for the last condition is to avoid Corollary 1 which is met for direct sum of repetition codes). By analogy with [3] (where maximum values of $M(C)$ were

2010 *Mathematics Subject Classification.* Primary 94A10; Secondary 05C38,05B35.
Key words and phrases. minimal codewords, matroid theory, cycle code of graphs.
1. Corresponding author Ph. +64 3 4797766, e-mail: raldred@maths.otago.ac.nz.

considered), we define

$$m(n,k) = \min\{M(C) : C \in \mathbf{C}[n,k]\},$$

as the minimum of $M(C)$ over that set of codes. Similarly we define $m_g(n,k)$ by restricting the set of codes considered to be cycle codes of graphs.

2. Matroid bounds

In the following, we translate results from matroids to codes by considering the matroid of linear dependence of the columns of the parity-check matrix of the code. Thus this matroid, when thought of as an $[n,k]-$ code, has n points and rank $n-k$. The circuits of the matroid correspond bijectively to the minimal codewords of the code. The matroid is called **simple** if its has no loops (single element dependent sets) nor parallel elements (two element dependent sets). This is equivalent to the code having distance at least three. Such codes are sometimes called **projective.** When the code is the cycle code of a connected graph on p vertices with q edges, the minimal codewords correspond to cycles and the parameters of the cycle code are $[q, q-p+1]$ with dual distance equal to the edge-connectivity of the graph, that is, the smallest number of edges that must be deleted in order to make the graph disconnected.

Theorem 1. *(Dosa, Szalkai, Laflamme* [9]*) Any matroid M of size μ and rank ν has at least $\mu - \nu$ circuits.*

This implies the following.

Corollary 1. *Any [n,k] code C satisfies $M(C) \geq k$.*

Below is a purely coding-theoretic proof of Corollary 1.

Proof: By [4, Lemma 2.1] we know that the $M(C)$ minimal vectors span C, a vector space of dimension k. Therefore elementary linear algebra ensures that $M(C) \geq k$. □

The inequality in Corollary 1 is an equality for repetition codes.

Theorem 2. *(Dosa, Szalkai, Laflamme* [9]*) Any loopless matroid M of size μ and rank ν has at least $b\binom{a+1}{2} + (\nu - b)\binom{a}{2}$ circuits, where a, b are the quotient and remainder of μ by ν.*

This, too, has a corollary for linear codes.

Corollary 2. *Any $[n,k]-$ code C of distance at least 2 satisfies*

$$M(C) \geq b\binom{a+1}{2} + (n-k-b)\binom{a}{2},$$

where a, b are the quotient and remainder of n by $n-k$.

For graphs this implies:

Corollary 3. *Any 2-edge-connected graph with p vertices and q edges contains at least*

$$b\binom{a+1}{2} + (p-1-b)\binom{a}{2},$$

cycles where a, b are the quotient and remainder of q by $p-1$.

The bound in Corollary 3 is tight. Consider for example a tree on p vertices where each edge is replaced by three edges. This graph has $q = 3(p-1)$ edges and contains $3(p-1)$ cycles. For this graph the inequality in Corollary 3 is an equality with $a = 3$ and $b = 0$.

Dosa, Szalkai, Laflamme [9] suggested to sharpen the bounds of Theorem 1 and Theorem 2 for a loopless matroid without parallel elements. We first point out that a result by Kashyap [12] on codes can be extended to matroids. Then we consider graphic matroids.

3. Matroids with no loops and parallel edges

Theorem 3. *Any loopless matroid M of size μ and rank ν without parallel elements has at least μ cocircuits.*

Proof: Consider the lattice $L(M)$ of flats (maximal closed sets) of M. Let W_r be the number of elements in $L(M)$ of rank r (W_r is a so-called Whitney number of the second kind).

Thus the number of cocircuits of M is equal to $W_{\nu-1}$.

By the result of Greene [10] we have

$$W_{\nu-1} \geq W_1,$$

where W_1 is the number of elements in $L(M)$ of rank 1 (points of $L(M)$). Equivalently, it is the number of flats of M of rank 1. Since M is simple, we conclude that $W_1 = \mu$. □

Corollary 4. *(Kashyap* [12]*) Any [n,k] code C of dual distance at least* 3 *satisfies $M(C) \geq n$.*

Note that our proof of Theorem 3 is purely combinatorial while Kashyap's arguments are geometric.

Corollary 5. *Any 3-edge-connected graph with q edges contains at least q cycles.*

The examples showing that the Corollary 3 is best possible also show that Corollary 5 is best possible. However, Theorem 4 in the next section shows that the right bound is a quadratic function of q if we exclude cutvertices.

4. Graph bounds

Recall that a connected graph is **k-edge-connected**, respectively **k-connected**, if the smallest number of edges, respectively vertices, that must be deleted in order to make the graph disconnected is at least k. (If any two vertices are joined by at least one edge, then it is not possible to make the graph disconnected by deleting vertices. In that case the requirement for being k-connected is that the graph has at least $k+1$ vertices.) A 2-connected graph may have multiple edges whereas, by convention, a 3-connected graph does not.

Lemma 1. *Let G be a 2-connected graph with q edges and p vertices. Let e be an edge of G. Then G has at least q-p+1 cycles which contain e.*

Proof: We proceed by induction on $q+p$. The smallest 2-connected graph is K_3, where $p+q=3+3=6$ and there is a cycle through any edge so the result is true in this case. If G contains a vertex v of degree 2, then we replace v and its two incident edges by one edge and use induction. If all vertices have degree at least 3, then G contains an edge e' distinct from e such that $G-e'$ is 2-connected. (This is well known and easy to prove by the following argument: Let H be a 2-connected proper subgraph of G which contains e. If H is chosen to be maximal under these conditions, then it is easy to see that G has only one edge which is not in H.) By the induction hypothesis, $G-e'$ has at least $q-p$ cycles containing e. But, G also has at least one cycle containing e, e'. Hence G has at least $q-p+1$ cycles which contain e. □

The next result implies Corollary 3 although it has a slightly stronger hypothesis.

Theorem 4. *Let G be a 2-connected graph with q edges and p vertices. Then G has at least $\binom{q-p+2}{2}$ cycles.*

Proof: We use induction on $q+p$. Again, the result is clearly true for K_3. If G contains a vertex v of degree 2, then we replace v and its two incident edges by one edge and use induction. If all vertices have degree at least 3, then G contains an edge e such that $G-e$ is 2-connected. By Lemma 1, G has at least $q-p+1$ cycles which contain e. By the induction hypothesis (applied to $G-e$), the graph G has at least $\binom{q-p+1}{2}$ cycles which do not contain e. Hence G has at least $\binom{q-p+2}{2}$ cycles. □

Example: The inequality of Theorem 4 is an equality for the following graph: two vertices joined by $q-p+2$ edges along with $p-2$ additional vertices of degree 2 inserted on the edges.

Remark: Theorem 4 implies Corollaries 3 and 5 immediately by induction on p. For, if the graph under consideration is 2-connected, we apply Theorem 4. Otherwise there is a cutvertex v, and hence we can write the graph as the union of two graphs having precisely v in common. Then we apply induction to these two subgraphs.

5. The smallest number of cycles in 3-connected graphs

Let $f_k(p,q)$ be the smallest number of cycles in a k-connected graph with p vertices and q edges. One would think that if p is fixed, then the function increases as a function of q. But it does not. Indeed, the wheel, defined below, shows that $f_3(p, 2p-2)$ is at most a quadratic polynomial of p. But $f_3(p, 3p/2)$ is superpolynomial as proved in [2]. In this section we prove that, for $p \geq 38$, every 3-connected graph on p vertices distinct from the wheel has more cycles than the wheel on p vertices.

The **wheel** with p vertices is obtained from a cycle with $p-1$ vertices by adding a vertex joined to all vertices of the cycle. That vertex of degree $p-1$ is called the **center** of the wheel. Two edges are called **independent** if they have no end in common.

Let G be a 3-connected graph and $e \in E(G)$. Barnette and Grünbaum [6] and Titov [19] considered the following operation.

(1) Delete e from G to get $G-e$.
(2) If some endvertices of e have degree two in $G-e$, then *suppress* them (i.e. delete the vertex of degree two and add an edge between the two neighbours of the deleted vertex) to get $G \triangle e$.
(3) If multiple edges occur in $G \triangle e$, then replace them by single edges. (Recall that a 3-connected graph has no multiple edges.)

The resulting graph is denoted by $G \ominus e$. If $G \ominus e$ is 3-connected, then e is said to be **removable**. If e is removable in G and $f \in E(G)$ meets e at a vertex v of degree 3, then the edge in $G \ominus e$ corresponding to f after suppressing v will also be denoted f.

The proof of the following lemma can be obtained by a slight modification of the proof by Thomassen [21, Lemma 4.1].

Lemma 2. *Let G be a 3-connected graph and let H be a proper subgraph which is a subdivision of a 3-connected graph. Then G has a removable edge e such that $G-e$ contains H.*

Jianji [11] proved the following.

Theorem 5. *Let G be a 3-connected graph with $p \geq 5$ vertices. If G is not isomorphic to the wheel on 5 or 6 vertices, then G has at least $(3p+18)/7$ removable edges.*

We shall also use the following fundamental result of Lovász.

Lemma 3. [14, Exercise 6.67] *Let G be a 3-connected graph and e, f, g be three distinct edges. Then G has a cycle containing all of e, f and g unless either $G - \{e, f, g\}$ is disconnected or e, f, g are all incident on a common vertex.*

We recall the definition of cycle code (cycle space) of a graph. If G is a graph, then the set of all subsets of edges may be thought of as a vector space over the field with two elements where addition is the symmetric difference. The *cycle space* $Z(G)$ is the subspace generated by the cycles. If G is connected and has p vertices and q edges, then the cycle space has dimension $q-p+1$. If e_1, e_2 are edges of G such that G has a cycle containing precisely one of these edges, then the cycles containing both of e_1, e_2 generate a subspace which is a proper subspace of $Z(G)$, that is, it has dimension at most $q-p$.

Theorem 6. *Let G be a 3-connected graph with p vertices, and let e_1, e_2 be independent edges of G. Let G' be obtained from G by replacing some edges other than e_1, e_2 by multiple edges. If $G-e_1-e_2$ has a bridge, then that bridge is also a bridge in $G'-e_1-e_2$ (that is, it is not made into a multiple edge.) Let q be the number of edges in G'. Then the cycles in G' containing both e_1 and e_2 generate a subspace of the cycle space of dimension $q-p$.*

Proof: : The proof is by induction on q. The theorem is easily verified for the smallest 3-connected graph which is the complete graph on four vertices. So assume that $q \geq 7$. For $p = 5$, the statement is easily verified because the only 3-connected graphs on 5 vertices are the wheel, the complete graph K_5 and K_5 minus an edge. So assume that $p \geq 6$.

If the edge f is part of a multiple edge, then we apply induction to $G' - f$. The resulting cycle space has dimension $q - 1 - p$. By Lemma 3, G' has at least one cycle containing e_1, e_2, f. That cycle is not a linear combination of cycles in $G' - f$. So assume that G' has no multiple edges, that is, $G' = G$.

It is easy to verify the statement for the wheel with 6 vertices. So assume that G is not that wheel. By Theorem 5, G has at least 6 removable edges. At least four of these, say e_3, e_4, e_5, e_6 are distinct from e_1 and e_2.

We consider first the case where G has a removable edge f such that e_1, e_2 are independent edges in $G \triangle f$, and e_1, say, is part of a double edge in $G \triangle f$. That is, f has an end v of degree 3 joined to the two ends x_1, y_1 of e_1. Now we consider the edge $f' = x_1 v$ instead of f. Then f' is removable in G, and we can apply induction to $G \triangle f'$ because e_1, e_2 are independent in $G \triangle f'$, and $G \triangle f'$ has at most one double edge, and that double edge is incident with e_1. By induction, $G \triangle f'$ has $(q-2)-(p-1) = q-p-1$ distinct cycles through e_1 and e_2. By Lemma 3, there is a cycle in G through e_1, e_2 and f' and thus the cycle space of G has dimension $q - p$ as required.

We consider next the case where G has a removable edge f such that e_1, e_2 are independent edges in $G \triangle f$, neither of e_1, e_2 is part of a double edge, and $G \triangle f - e_1 - e_2$ has no double edge which becomes a bridge in $G \ominus f - e_1 - e_2$. Then the cycles in $G \triangle f$ containing both e_1 and e_2 span a space of dimension $q - p - 1$, by the induction hypothesis. By Lemma 3, G has at least one cycle containing e_1, e_2, f. Hence the cycles in G containing both e_1 and e_2 span a space of dimension $q - p$.

Consider now the case where G has a removable edge f such that e_1, e_2 are independent edges in $G \triangle f$, and $G \triangle f$ has a double edge which becomes a bridge e_3 in $G \ominus f - e_1 - e_2$. That is, f has an end v of degree 3 joined to the two ends of e_3. By induction, the cycles in $G - v$ containing both e_1 and e_2 span a space of dimension $q - p - 2$. By Lemma 3, G has at least one cycle C containing e_1, e_2, f. It is easy to modify this cycle into a cycle C' containing e_1, e_2, f such that one of C, C' contains e_3 and the other does not. Adding C, C' to the space of dimension $q - p - 2$ increases the dimension by 2.

So we may assume that, for each removable edge f, the edges e_1, e_2 have a common end in $G \ominus f$. In particular, each of e_3, e_4, e_5, e_6 has an end of degree 3 in common with one of e_1, e_2. Let $e_i = x_i y_i$ for $i = 1, 2, 3, 4, 5, 6$.

Consider now the case where e_1, e_2 are contained in a 4-cycle, say $C : x_1 y_1 y_2 x_2 x_1$. Let x be a vertex not in this 4-cycle C. By Menger's theorem there are three internally disjoint paths P_1, P_2, P_3 from x to C, say to x_1, y_1, y_2. (Internally disjoint means that they have only x in common pair by pair.) Let P_4 be a path in $G - x_1 - y_2$ from x_2 to $P_1 \cup P_2 \cup P_3$. The resulting graph H is a subdivision of a 3-connected graph H'. If H is a proper subgraph of G then, by Lemma 2, G has a removable edge f outside this subgraph. This contradicts the assumption that e_1, e_2 have a common end in $G \ominus f$. If $H = G$, then $G = H = H'$ has five or six (hence six)

vertices in which case it is easy to find the dimension of the space generated by the cycles through e_1, e_2. So, we may assume that e_1, e_2 are not contained in a 4-cycle.

We say that a removable edge distinct from e_1, e_2 is *internal* if it joins two ends of e_1, e_2 and *external* otherwise. As e_1, e_2 are not contained in a 4-cycle, there are at most two internal edges and hence at least two external edges. Consider now an external edge, say e_3. Then e_3 has an end $x_3 = x_1$ in common with e_1 but no end in common with e_2. As e_1, e_2 have an end in common in $G \ominus e_3$, it follows that x_1 has degree 3 and is joined to one of x_2, y_2. Since this argument holds for every external edge, and since e_1, e_2 are not contained in a 4-cycle, it follows that there are at most two external edges. If follows that there are precisely two internal edges and precisely two external edges. Thus the notation can be chosen such that e_5, e_6 are the edges x_2x_1, x_2y_1 and the external edges are $e_3 = x_1y_3$ and $e_4 = y_1y_4$. Since there are at least six removable edges, there are precisely six removable edges, namely $e_1, e_2, e_3, e_4, e_5, e_6$. But, then e_2 cannot be removable because x_1, y_2 have degree 2 in the 3-connected graph $G \ominus f$, a contradiction which proves Theorem 6. □

Corollary 6. *Let G be a 3-connected graph with p vertices and q edges, and let e_1, e_2 be independent edges of G. Then G has at least $q - p$ cycles containing both e_1 and e_2. In particular, G has at least $\lceil p/2 \rceil$ cycles containing both e_1 and e_2.*

The bound $q-p$ in Corollary 6 cannot be increased to $q-p+1$ as shown by two independent edges in the wheel with p vertices where one of the edges is incident with the center.

Lemma 4. *Let G be a 3-connected graph on p vertices, and let e be an edge of G. If both ends of e have degree precisely 3, then G has at least $(\lceil p/2 \rceil^2 + \lceil p/2 \rceil)/2 + 1$ cycles containing e.*

Proof: (by induction on p) We leave the cases $p = 4, 5$ and the wheel on 6 vertices for the reader. Assume that $p \geq 6$ and G is not the wheel on 6 vertices.

By Theorem 5, G has at least 6 removable edges. So G has a removable edge f such that e, f have no end in common. Now $G \ominus f$ has at least $p - 2$ vertices so, by induction, $G \ominus f$ has at least $(\lceil (p-2)/2 \rceil^2 - \lceil (p-2)/2 \rceil)/2 + 1$ distinct cycles containing e. By Corollary 6, G has at least $\lceil p/2 \rceil$ cycles containing both e and f so G has at least $(\lceil p/2 \rceil^2 + \lceil p/2 \rceil)/2 + 1$ distinct cycles containing e. □

Lemma 5. *Let G be a 3-connected graph on p vertices. If G is not isomorphic to a wheel, then for each edge e, G has at least $3p - 14$ cycles containing e.*

Proof: Let a_p be defined recursively by $a_4 = 4$, $a_5 = 7$ and $a_p = \min(a_{p-2} + \lceil p/2 \rceil, a_{p-1} + 3)$ for $p \geq 6$.

We prove, by induction on p, that G has at least a_p distinct cycles containing e. As $a_p \geq 3p - 14$ for all $p \geq 5$, this implies the theorem.

The smallest 3-connected graph which is not a wheel is the complete graph with 5 vertices minus an edge. It has more than $7 = a_5$ cycles through every edge. The same is also true for K_5 itself.

So, we may assume that $p \geq 6$. Let $f \neq e$ be a removable edge of G. By Theorem 5, G has at least six removable edges. Thus f can be chosen in such a way that either f is not incident with an end of e, or f is incident with an end of e which has

degree > 3. Hence $G \ominus f$ has at least $p-2$ vertices when e and f have no common end, and $G \ominus f$ has at least $p-1$ vertices otherwise.

Suppose that $G \ominus f$ is a wheel. If e is not incident with the center of the wheel, then $G \ominus f$ has at least $\binom{p-3}{2} + 1 \geq 3p - 14$ cycles containing e. Assume therefore that e is incident with the center v of the wheel. As G is not a wheel, $G - v$ is a 2-connected graph which is not a cycle. Thus for each edge $g \neq e$ incident with v, $G - v$ has three distinct paths between the ends of e, g other than v, so that G has at least $3(p-4) > 3p - 14$ cycles through e. Therefore we may assume that $G \ominus f$ is not a wheel.

If e and f are independent, then by Corollary 6, G has at least $\lceil p/2 \rceil$ distinct cycles containing both e and f. As $G \ominus f$ has at least a_{p-2} cycles containing e it follows that G has at least $\lceil p/2 \rceil + a_{p-2} \geq a_p$ cycles containing e. So assume that e and f have a common end v. Hence $G \ominus f$ has at least $p-1$ vertices.

Since G is not isomorphic to a wheel, $G - v$ is a 2-connected graph which is not a cycle. Therefore $G - v$ has at least three distinct paths between the ends of e, f other than v. Thus G has at least three cycles containing e and f. By induction, $G \ominus f$ has at least a_{p-1} cycles containing e, and hence G has at least $3 + a_{p-1} \geq a_p$ cycles through e.

□

Lemma 5 is close to best possible. In [16] the lower bound $3p - 14$ is replaced by $3p - 11$ if $p \neq 8$ which is best possible. For $p = 8$ there is an example showing that the correct bound is $12 = 3p - 12$.

By combining Lemmas 2, 4, 5 we can prove that for large order, the wheels have the minimum number of cycles among 3-connected graphs with the same order. Examples show that this does not extend to 3-connected graphs with few vertices, but we do not know the smallest order for which it holds.

Theorem 7. *Let G be a 3-connected graph on p vertices. If $p \geq 38$, and G is not a wheel, then the number of cycles in G is greater than the number of cycles in the wheel on p vertices.*

Proof: Let $w_p = p^2 - 3p + 3$ be the number of cycles in the wheel on p vertices. We define $c_4 = 7, c_5 = 13$. For each $p \geq 6$, we let c_p be the minimum of the following three numbers:

(1) $c_{p-2} + (\lceil p/2 \rceil^2 + \lceil p/2 \rceil)/2 + 1$
(2) $c_{p-1} + 3p - 14$
(3) w_p

Using Lemmas 2, 4, 5, we prove by induction that every 3-connected graph on p vertices has at least c_p cycles.

As $w_p = w_{p-1} + 2p - 4$ it follows immediately that $c_p = w_p$ for p sufficiently large. 38 is the smallest p for which this is true. A close inspection of the proof shows that G has strictly more than w_p cycles unless G is a wheel.

□

6. A general lower bound on the number of cycles in 3-connected graphs with p vertices and q edges

Thomassen [20] proved that the vertex set of a simple graph G (that is, a graph without multiple edges) with minimum degree at least $12d$ can be divided into two nonempty sets A, B such that the subgraphs $G(A), G(B)$, induced by A, B, respectively, have minimum degree at least d. Subsequently, Stiebiz [15] proved the conjecture in [20] that the same conclusion holds if the minimum degree of G is at least $2d+1$ (and this is best possible).

Kostochka [13] and Thomason [17] independently proved that a simple graph with p vertices and q edges contains a subgraph which can be contracted into a complete graph with m vertices provided q is at least a constant times $pm\sqrt{\log m}$. Subsequently, Thomason [18] proved that the condition

$$q > (0.319... + o(1))pm\sqrt{\log m}$$

suffices (and this is essentially best possible).

Theorem 8. *Let G be a 3-connected graph with p vertices, q edges and average degree $d = 2q/p$. Then for each $\epsilon > 0$ and for sufficiently large d, the number of cycles in G is at least $\lfloor (3d/8)^{1-\epsilon} \rfloor ! p/2$.*

Proof: We delete successively vertices of degree at most q/p from G until we get a graph G', say, of minimum degree $d' > p/q = d/2$. By the result in [15] the vertex set of G' can be divided into sets A, B such that each of the graphs $G'(A), G'(B)$ have minimum degree at least $d'/2 - 1 > d/4 - 1$. Assume that A is no larger than B, that is, A has at most $p/2$ vertices. By the result in [18], for sufficiently large d, $G(A)$ has a subgraph H which can be contracted into a complete graph with m vertices where $m > (3d/8)^{1-\epsilon}$. That is, H contains m pairwise disjoint connected subgraphs such that any two of these connected subgraphs are joined by at least one edge. We choose H to be minimal with these properties. Then the disjoint subgraphs are trees and any endvertex of each tree is joined by an edge to another tree. Moreover, if x, y are any two distinct vertices in H, then H has at least $(m-2)!$ paths from x to y.

Consider now a connected component C of $G - V(H)$, and let C' be the graph obtained from G by removing all the vertices not in $H \cup C$ and then adding edges to H so that it becomes complete. We may assume that $|V(H)| > 2$, and hence C' is 3-connected.

We claim that C' has at least $|V(C)|$ distinct H-paths, i.e. paths such that only their ends are in H.

We prove this claim by induction on $|V(C)| + |E(C)|$. The claim is trivial for $|V(C)| = 1$. Apply Lemma 2 to C', H and let e be the resulting removable edge. Then it is easy to prove the claim applying induction hypothesis on $C' - e$ since there are at least two H-paths containing e.

As each of these H-paths can be extended to $(m-2)!$ distinct cycles in G, the proof is complete. □

7. Open problems

Open Problem 1. *What is the smallest number that can replace* 38 *in Theorem 7 ?*

Open Problem 2. *Can the term p in Theorem 8 be replaced by a quadratic function of p ?*

The wheel shows that a quadratic function of p is the best we can hope for in general. However, if the average degree d is large, say $d > 100$, then perhaps p could be replaced by a cubic function. That would be best possible as shown by the following example: Take a collection of disjoint copies of the complete graph with $d+1$ vertices. Select a triangle in each of them and identify all those selected triangles.

Open Problem 3. *Does Theorem 8 extend to* 2*-connected graphs?*

8. Tables

We have produced tables providing values (ranges of values) for $m(n.k)$ and $m_g(n,k)$ for small values of n,k. By decreasing values of k we look at the values of $m(n,k)$. The quantity $m(n,k)$ becomes undefined when there are no codes of dual distance ≥ 3 for these values of n and k.

The following Proposition is helpful in our computations.

Proposition 1. *If $m(n,k) = n$, then for every integer T we have*

$$m(n+T, k+T) = n+T.$$

Proof: Let C be an $[n,k]$-code of dual distance at least 3 such that $M(C) = m(n,k) = n$. Take the direct sum with an universe code of length T. Specifically

$$D = C \oplus \mathbb{F}_2^T.$$

Thus D is an $[n+T, k+T]-$code. Then $M(D) = M(C) + T = n+T$. Thus $m(n+T, k+T) \leq M(D) = n+T$, and by Kashyap bound the result follows. □

The following values are immediate.

- $m(n,n)$ is undefined.
- $m(n,n-1) = n$ since $M(C) = 3$ for $C = R_3^{\perp}$ where R_m denotes the repetition code of length m.
- $m(n,n-2) = n$, for $n \geq 6$ since there is a $[6,4]$ code C_6 with dual distance 3 and $M(C_6) = 6$, eg $C_6 = R_3^{\perp} \oplus R_3^{\perp}$.
- $m(n,k)$ is undefined for $k \leq 1$.

Tables 1 and 2 show values and bounds for $m(n,k)$ while Table 3 shows values for $m_g(n,k)$ for $1 \leq n \leq 15$. Lower bounds are given by the Kashyap bound while upper bounds are obtained by explicit codes. The values were computed using MAGMA [8]. We also used the graph generation program NAUTY of B. Mckay [22] in the computations for Table 3. A blank entry means that $m(n,k)$ or $m_g(n,k)$ is undefined.

n/k	1	2	3	4	5	6	7	8	9
3		3							
4			4						
5			5-6	5					
6			6-7	6	6				
7			7	7-8	7	7			
8				8	8-9	8	8		
9				9-12	9	9	9	9	
10				10-14	10	10	10	10	10
11				11-14	11-15	11	11	11	11
12				12-15	12-15	12-13	12	12	12
13				13-15	13-16	13-14	13	13	13
14				14-15	14-16	14	14-18	14	14
15				15	15-24	15-25	15	15-22	15

TABLE 1. $m(n, k)$ for $3 \leq n \leq 15, 1 \leq k \leq 9$

n/k	10	11	12	13	14	15
10						
11	11					
12	12	12				
13	13	13	13			
14	14	14	14	14		
15	15	15	15	15	15	

TABLE 2. $m(n, k)$ for $10 \leq n \leq 15, 10 \leq k \leq 15$

n/k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3															
4															
5															
6			7												
7															
8				13											
9				14	22										
10					21	37									
11					22	30									
12					26	14	52								
13						30	39	85							
14						38	20	65	133						
15						46	21	29	103	197					

TABLE 3. $m_g(n, k)$ for $3 \leq n \leq 15$

9. Acknowledgement

This paper was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, under grant No. (33-3/1432/HiCi). The authors, therefore, acknowledge with thanks DSR technical and financial support.

References

[1] E. Agrell, On the Voronoi neighbor ratio for binary linear codes, IEEE Transactions in Information Theory (1998) 3064–3072.

[2] R.E.L. Aldred, C Thomassen, On the number of cycles in 3-connected cubic graphs, J. Combinatorial Theory Ser. B 71 (1997) 79–84.

[3] A. Alahmadi, R.E.L. Aldred, R. de la Cruz, P. Solé, C. Thomassen, The maximum number of minimal codewords in long codes, *Discrete Applied Mathematics*, **161**(2013) 424 -429.

[4] A. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Transactions in Information Theory (1998) 2010–2017.

[5] A. Ashikhmin, A. Barg, G. Cohen, L. Huguet, Variations on minimimal codewords in linear codes, Springer LNCS 948 (1995) 96–105.

[6] D. Barnette and B. Grünbaum, On Steinitz's theorem concerning convex 3-polytopes and on some properties of planar graphs, The Many Facets of Graph Theory, Lecture Notes in Math., vol. 110, Springer-Verlag, Berlin, 1969, pp. 27–40.

[7] A. Betten, Distance optimal indecomposable codes over GF(2), `http://www.math.colostate.edu/~betten/research/codes/GF2/codes_GF2.html`

[8] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997) 235–265.

[9] Gy. Dosa, I. Szalkai, C. Laflamme, The maximum and minimum number of circuits and bases of matroids, PU. M. A. **15** (2004) 383–392.

[10] C. Greene, A Rank Inequality for Finite Geometric Lattices, J. Combinatorial Theory 9 (1970) 357–364.

[11] S, Jianji, The number of removable edges in 3-connected graphs, J. Combinatorial Theory Ser. B 75 (1999) 74-87

[12] N. Kashyap, On the convex geometry of binary linear codes, preprint. `http://www.ece.iisc.ernet.in/~nkashyap/Papers/code_geometry.pdf`

[13] A.V. Kostochka, A lower number for the Hadwiger number of graphs by their average degree, Combinatorica 4 (1984) 307–316.

[14] L. Lovász, Combinatorial problems and exercises, North Holland, 1979.

[15] M. Stiebitz, Decomposing graphs under degree constraints, J. Graph Theory 23 (1996) 321–324.

[16] S. Ok, Ph.D. Thesis, Technical University of Denmark, 2015, preprint.

[17] A. Thomason, An extremal number for contractions of graphs, Math. Proc. Cambridge Philos. Soc. 95 (1984) 261–265.

[18] A. Thomason, The extremal function for complete minors, J. Combinatorial Theory Ser. B 81 (2001) 318–338.

[19] V. K. Titov, A constructive description of some classes of graphs, Doctoral dissertation, Moscow, 1975.

[20] C. Thomassen, Graph decomposition with constraints on the connectivity and minimum degree, J. Graph Theory 7 (1983) 165–167.

[21] C. Thomassen, Kuratowski's theorem, J. Graph Theory 5 (1981) 225–241.

[22] B. D. McKay and A. Piperno, Practical Graph Isomorphism, II, J. Symbolic Computation (2013) 60 94-112.

Math Dept of King Abdulaziz University, Jeddah, Saudi Arabia
E-mail address: adelnife2@yahoo.com

Department of Mathematics and Statistics, University of Otago, P. O. Box 56, Dunedin, New Zealand
E-mail address: raldred@maths.otago.ac.nz

Division of Mathematical Sciences, SPMS, Nanyang Technological University, Singapore, and, Institute of Mathematics, University of the Philippines Diliman, Quezon City, Philippines
E-mail address: ROMA0001@e.ntu.edu.sg

Department of Mathematics, Technical University of Denmark, DK-2800 Lyngby, Denmark
E-mail address: seongmin.ok@gmail.com

Telecom ParisTech, 46 rue Barrault, 75634 Paris Cedex 13, France., and, Math Dept of King Abdulaziz University, Jeddah, Saudi Arabia
E-mail address: sole@enst.fr

Department of Mathematics, Technical University of Denmark, DK-2800 Lyngby, Denmark, and, Math Dept of King Abdulaziz University, Jeddah, Saudi Arabia
E-mail address: ctho@dtu.dk